



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/566,728	02/02/2006	Tomoaki Ryu	11900618PUS1	9704
2292 7590 03/09/2009 BIRCH STEWART KOLASCH & BIRCH PO BOX 747 FALLS CHURCH, VA 22040-0747				
EXAMINER				
POOMORE, TRAVIS D				
ART UNIT		PAPER NUMBER		
2436				
NOTIFICATION DATE		DELIVERY MODE		
03/09/2009		ELECTRONIC		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

Office Action Summary

Application No.

10/566,728

Applicant(s)

RYU, TOMOAKI

Examiner

Travis Pogmore

Art Unit

2436

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 February 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-11 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-11 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SE/US)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. This action is in response to the request for reconsideration filed February 13, 2009.
2. Claims 1-11 are currently pending. Claims 6 and 9 have been previously presented. Claims 1-4 and 7 are amended.
3. Applicant's arguments, with regards to claims 1-11, filed February 13, 2009 have been fully considered but they are not persuasive.

Examiner Notes

4. Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.
5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Objections

6. Applicant's arguments, see page 9, and respective amendments with respect to the improper form of claim 3 have been fully considered and are persuasive. The objection thereof has been withdrawn.

Claim Rejections – 35 USC § 112

7. Applicant's arguments, see page 9, with respect to the indefiniteness of claims 1, 2, 5 and 8 have been fully considered and are persuasive. The § 112 rejections thereof have been withdrawn.

Claim Rejections – 35 USC § 103

8. Claims 1-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 4,907,275 (hereinafter "Hashimoto") in view of U.S. Patent No. 5,392,351 (hereinafter "Hasebe") in further view of U.S. Patent No. 7,230,898 (hereinafter "Yokota").

As to claim 1, Hashimoto teaches a digital recording apparatus comprising:

a data control circuit which receives a digital recording signal (Fig. 1, elements 17 and 19);

a memory which is capable of communicating information with the data control circuit (Fig. 1, elements 14 and 16);

an encryption circuit which is capable of communicating information with the data control circuit, the encryption circuit encrypting the digital recording signal (Fig. 1, element 4); and

a recording signal processing circuit which causes the data control circuit to control transmission of the digital recording signal (Fig. 2a, element 10, the CPU of the computer system);

wherein when the digital recording signal needs to be encrypted, the encryption circuit begins to start up and the digital recording signal is transmitted from the data control circuit to the memory to be stored in the memory during start-up of the encryption circuit, and when the encryption circuit becomes capable of operation, the digital recording signal stored in the memory is transmitted via the data control circuit to the encryption circuit and is encrypted by the encryption circuit to be recorded in a recording unit (column 3, lines 1-15, since the purpose of a buffer is to store data after it is transferred but before it can be processed (either due to the circuit not having completed start-up or it is currently processing other data)), but does not specifically teach the recording unit which is controlled by the data control circuit, the recording unit recording the digital recording signal on a recording medium, nor the encryption circuit being deactivated before the data control circuit receives the digital recording signal to be encrypted.

However, Hasebe teaches a recording unit which is controlled by the data control circuit, the recording unit recording the digital recording signal on a recording medium is well known and expected in the art (Fig. 4, element S6, column 9, line 66 to column 10,

line 15, in order to record encrypted information on the storage medium it must inherently have a recording unit).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to record the signal on a recording medium as in Hasebe because this is a well known and expected addition to general purpose computers.

Furthermore, Yokota teaches the encryption circuit being deactivated before the data control circuit receives the digital recording signal to be encrypted (column 16, lines 32-38).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to activate the encryption circuit only as needed as in Yokota because this "translates into a reduction of power consumption ... [and] when this embodiment operates from a battery unit, the process helps prolong the life of the battery" (Yokota, column 16, lines 39-42).

As to claim 2, Hashimoto teaches a digital reproducing apparatus comprising:

- a data control circuit which controls the reproducing unit and outputs a reproduced digital recording signal (Fig. 2a, element 10, the CPU controlling every part of the computer system);
- a memory which is capable of communicating information with the data control circuit (Fig. 1, elements 14 and 16);

a decryption circuit which is capable of communicating information with the data control circuit, the decryption circuit decrypting the digital recording signal (Fig. 1, element 4 and column 1, lines 52-58, as substantially similar hardware and process is used for decryption the encryption circuit also acts as a decryption circuit); and

a recording signal processing circuit which causes the data control circuit to control transmission of the digital recording signal (Fig. 2a, element 10, the CPU);

wherein when the digital recording signal encrypted and recorded on the recording medium needs to be decrypted and reproduced, during start-up of the decryption circuit, the digital recording signal having been stored before start-up of the decryption circuit is outputted via the data control circuit, and when the decryption circuit is capable of operation, the digital recording signal read by the reproducing unit is transmitted via the data control circuit to the decryption circuit and is decrypted by the decryption circuit to be outputted (column 3, lines 1-15, since the purpose of a buffer is to store data after it is transferred but before it can be processed (either due to the circuit not having completed start-up or it is currently processing other data)), but does not teach a reproducing unit which reproduces a digital recording signal from a recording medium, nor the decryption circuit being deactivated before the data control circuit receives the digital recording signal to be encrypted.

However Hasebe teaches a reproducing unit which reproduces a digital recording signal from a recording medium (column 9, line 66 to column 10, line 15, the reproducing unit comprising the "optical magnetic apparatus" for the appropriate medium of an "optical magnetic disk").

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to reproduce a signal from a recording medium as in Hasebe because his is a well known and expected addition to general purpose computers.

Furthermore, Yokota teaches the decryption circuit being deactivated before the data control circuit receives the digital recording signal to be encrypted (column 16, lines 32-38).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to activate the encryption circuit only as needed as in Yokota because this "translates into a reduction of power consumption ... [and] when this embodiment operates from a battery unit, the process helps prolong the life of the battery" (Yokota, column 16, lines 39-42).

As to claim 3, Hashimoto teaches a digital recording/reproducing apparatus comprising:

the digital recording apparatus of claim 1 (as taught by Hashimoto, Hasebe and Yokota above); and

a digital reproducing apparatus comprising:

a data control circuit which controls the reproducing unit and outputs a reproduced digital recording signal (Fig. 2a, element 10, the CPU controlling every part of the computer system);

a memory which is capable of communicating information with the data control circuit (Fig. 1, elements 14 and 16);

a decryption circuit which is capable of communicating information with the data control circuit, the decryption circuit decrypting the digital recording signal (Fig. 1, element 4 and column 1, lines 52-58, as substantially similar hardware and process is used for decryption the encryption circuit also acts as a decryption circuit); and

a recording signal processing circuit which causes the data control circuit to control transmission of the digital recording signal (Fig. 2a, element 10, the CPU);

wherein when the digital recording signal encrypted and recorded on the recording medium needs to be decrypted and reproduced, during start-up of the decryption circuit, the digital recording signal having been stored before start-up of the decryption circuit is outputted via the data control circuit, and when the decryption circuit is capable of operation, the digital recording signal read by the reproducing unit is transmitted via the data control circuit to the decryption circuit and is decrypted by the decryption circuit to be outputted (column 3, lines 1-15, since the purpose of a buffer is to store data after it is transferred but before it can be processed (either due to the circuit not having completed start-up or it is currently processing other data)), but does not teach a reproducing unit which reproduces a digital recording signal from a recording medium, nor the decryption circuit being deactivated before the data control circuit receives the digital recording signal to be encrypted.

However Hasebe teaches a reproducing unit which reproduces a digital recording signal from a recording medium (column 9, line 66 to column 10, line 15, the

reproducing unit comprising the "optical magnetic apparatus" for the appropriate medium of an "optical magnetic disk").

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to reproduce a signal from a recording medium as in Hasebe because his is a well known and expected addition to general purpose computers.

Furthermore, Yokota teaches the decryption circuit being deactivated before the data control circuit receives the digital recording signal to be encrypted (column 16, lines 32-38).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to activate the encryption circuit only as needed as in Yokota because this "translates into a reduction of power consumption ... [and] when this embodiment operates from a battery unit, the process helps prolong the life of the battery" (Yokota, column 16, lines 39-42).

As to claim 4, Hashimoto teaches an encryption apparatus comprising:

- a storage unit which stores a digital signal (Fig. 1, elements 14 and 16);
- an encryption unit which encrypts the digital signal (Fig. 1, element 4);
- a determination unit which determines whether or not the digital signal needs to be encrypted by the encryption unit (Fig. 1, elements 3 and 18, and column 6, lines 25-60, the logic circuit and the selector being the determination unit); and

a control unit which controls the storage unit and the encryption unit in such a way that when the determination unit determines that the digital signal does not need to be encrypted, the digital signal is not encrypted by the encryption unit and the digital signal stored in the storage unit is outputted, and when the determination unit determines that the digital signal needs to be encrypted, the digital signal from a time of the determination to a time when the enabling of the encryption unit is completed by the encryption key is stored in the storage unit and is encrypted by the encryption circuit to be outputted after the enabling of the encryption unit is completed (column 3, lines 1-15 and column 6, lines 25-60, since the purpose of a buffer is to store data after it is transferred but before it can be processed (either due to the circuit not having completed start-up or it is currently processing other data)), but does not specifically teach an encryption key generation unit which generates an encryption key for enabling the encryption unit, nor the encryption circuit being deactivated before the data control circuit receives the digital recording signal to be encrypted.

However Hasebe teaches an encryption key generation unit which generates an encryption key for enabling the encryption unit (column 4, lines 31-48, encryption being the role of the "vendor computer").

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to include a key generation unit as in Hasebe because this increases security by keeping all steps of the encryption process inside a single computer.

Furthermore, Yokota teaches the encryption circuit being deactivated before the data control circuit receives the digital recording signal to be encrypted (column 16, lines 32-38).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to activate the encryption circuit only as needed as in Yokota because this "translates into a reduction of power consumption ... [and] when this embodiment operates from a battery unit, the process helps prolong the life of the battery" (Yokota, column 16, lines 39-42).

As to claim 5, Hasebe teaches wherein the encryption key is generated from information read from a recording medium for recording the digital signal (column 4, lines 31-48).

As to claim 6, wherein when the determination unit determines that the digital signal needs to be encrypted, the storage unit secures a vacant capacity larger than a capacity capable of storing the digital signal from a time of the determination to a time when the enabling of the encryption unit is completed by the encryption key is well known and expected in the art (e.g. U.S. Patent No. 5,303,302, column 3, lines 40-59, in particular the third recited embodiment discloses a standard method of ensuring enough space to avoid a buffer overflow, and as in the invention described in Hashimoto, column 3, lines 1-15, the buffer must be able to store sufficient data for it to be correctly processed).

As to claim 7, Hashimoto teaches a decryption apparatus comprising:

a storage unit which stores a digital signal (Fig. 1, elements 14 and 16);

a decryption unit which decrypts an encrypted signal of the digital signal (Fig. 1, element 4 and column 1, lines 52-58, as substantially similar hardware and process is used for decryption the encryption circuit also acts as a decryption circuit);

a determination unit which determines whether or not the digital signal needs to be decrypted by the decryption unit (Fig. 1, elements 3 and 18, and column 6, lines 25-60, the logic circuit and the selector being the determination unit); and

a control unit which controls the storage unit and the decryption unit in such a way that when the determination unit determines that the digital signal does not need to be decrypted, the digital signal is not decrypted by the decryption unit and the digital signal stored in the storage unit is outputted, and when the determination unit determines that the digital signal needs to be decrypted, the digital signal from a time of the determination to a time when the enabling of the decryption unit is completed by the encryption key is stored in the storage unit and is decrypted by the decryption circuit to be outputted after the enabling of the decryption unit is completed (column 1, lines 52-58, column 3, lines 1-15 and column 6, lines 25-60, the decryption process being substantially the same as encryption, and since the purpose of a buffer is to store data after it is transferred but before it can be processed), but does not specifically teach an encryption key generation unit which generates an encryption key for enabling the

decryption, nor the decryption circuit being deactivated before the data control circuit receives the digital recording signal to be encrypted.

However Hasebe teaches an encryption key generation unit which generates an encryption key for enabling the decryption (column 4, lines 31-48, decryption being the role of the "user computer").

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to include a key generation unit as in Hasebe because this increases security by keeping all steps of the encryption process inside a single computer.

Furthermore, Yokota teaches the decryption circuit being deactivated before the data control circuit receives the digital recording signal to be encrypted (column 16, lines 32-38).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to activate the encryption circuit only as needed as in Yokota because this "translates into a reduction of power consumption ... [and] when this embodiment operates from a battery unit, the process helps prolong the life of the battery" (Yokota, column 16, lines 39-42).

As to claim 8, Hasebe teaches wherein the encryption key is generated from information read from a recording medium for recording the digital signal (column 4, lines 31-48).

As to claim 9, wherein when the determination unit determines that the digital signal needs to be decrypted, the amount of data of the digital signal stored in the storage unit is not less than an amount of data outputted from a time of the determination to a time when the enabling of the decryption unit is completed by the encryption key is well known and expected in the art (e.g. U.S. Patent No. 5,303,302, column 3, lines 40-59, in particular the third recited embodiment discloses a standard method of ensuring enough space to avoid a buffer overflow, and as in the invention described in Hashimoto, column 3, lines 1-15, the buffer must be able to store sufficient data for it to be correctly processed).

9. Claims 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hashimoto in view of Hasebe.

As to claim 10, Hashimoto teaches an encryption method comprising the steps of:

storing a digital signal (Fig. 1, elements 14 and 16);
encrypting the digital signal (Fig. 1, element 4); and
determining whether or not the digital signal needs to be encrypted (Fig. 1, elements 3 and 18, and column 6, lines 25-60, the logic circuit and the selector being the determination unit);

wherein when the determination is that the digital signal does not need to be encrypted, the digital signal is not encrypted and the stored digital signal is outputted,

and when the determination is that the digital signal needs to be encrypted, the digital signal from a time of the determination to a time when the function of encrypting is enabled is stored and is encrypted to be outputted after the enabling of the function of encrypting is completed (column 3, lines 1-15 and column 6, lines 25-60, since the purpose of a buffer is to store data after it is transferred but before it can be processed), but does not specifically teach generating an encryption key for enabling a function of encrypting the digital signal.

However, Hasebe teaches generating an encryption key for enabling a function of encrypting the digital signal (e.g. column 4, lines 31-48, encryption being the role of the "vendor computer").

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to generate a key as in Hasebe because this increases security by keeping all steps of the encryption process inside a single computer.

As to claim 11, Hashimoto teaches a decryption method comprising the steps of: storing a digital signal (Fig. 1, elements 14 and 16);
decrypting an encrypted digital signal of the digital signal (Fig. 1, element 4 and column 1, lines 52-58, as substantially similar hardware and process is used for decryption the encryption circuit also acts as a decryption circuit); and

determining whether or not the digital signal needs to be decrypted (Fig. 1, elements 3 and 18, and column 6, lines 25-60, the logic circuit and the selector being the determination unit);

wherein when the determination is that the digital signal does not need to be decrypted, the digital signal is not decrypted and the stored digital signal is outputted, and when the determination is that the digital signal needs to be decrypted, the digital signal from a time of the determination to a time when the function of decrypting is enabled is stored and is decrypted to be outputted after the enabling of the function of decrypting is completed (column 1, lines 52-58, column 3, lines 1-15 and column 6, lines 25-60, the decryption process being substantially the same as encryption, and since the purpose of a buffer is to store data after it is transferred but before it can be processed), but does not specifically teach generating an encryption key for enabling a function of decrypting the digital signal.

However, Hasebe teaches generating an encryption key for enabling a function of decrypting the digital signal (column 4, lines 31-48, decryption being the role of the "user computer").

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to generate a key as in Hasebe because this increases security by keeping all steps of the encryption process inside a single computer.

Response to Arguments

10. Applicant's arguments, with regards to claims 1-11, filed February 13, 2009 have been fully considered but they are not persuasive.

11. On page 9 of the Applicant's Response, Applicant argues that "examples of a recording medium are clearly disclosed in the specification" and requests that the 112 rejections of claims 1, 2, 5 and 8 should be withdrawn for that reason.

12. The Examiner agrees with Applicant's arguments and the 112 rejections thereof have been withdrawn.

13. On page 10 of the Applicant's Response, Applicant argues that Hashimoto fails to disclose or suggest "an encryption circuit that is deactivated ..." and the details of the operation when a digital recording signal needs to be encrypted within the limitations of claim 1.

14. The Examiner agrees with the Applicant's argument regarding this limitation, and as that limitation (and the corresponding limitations in claims 2-4 and 7) is the amended portion of the claim, the limitation has been addressed above by an additional reference (Yokota).

15. On pages 10-11 of the Applicant's Response, Applicant argues that Hashimoto fails to disclose or suggest the details of the operation when a digital recording signal needs to be encrypted. The Applicant further argues that Hashimoto does not disclose or suggest a particular purpose to the buffer. Finally, the Applicant accuses the Examiner of the use of impermissible hindsight in the reasoning for supporting the rejection.

16. The Examiner respectfully disagrees with the Applicant's arguments on all points. First, the details of the operation performed when a digital recording signal needs to be encrypted are taught by the buffer in Hashimoto (as listed in the original Office Action). The Examiner's statement regarding the purpose of a buffer is not merely a contention which needs to be taught or suggested by the prior art, but rather an inherent property of buffers. Second, the lack of Hashimoto in disclosing or suggesting the purpose (intended use) of a buffer is irrelevant as the functional capabilities of a buffer remains the same: temporarily storing data before it is used *for whatever reason*, including the instant applications stated (but unclaimed) purpose of "storing data due to the circuit not having complete start-up."

17. In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

18. Therefore, in view of the above reasons, Examiner maintains rejections.

Conclusion

19. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Travis Pogmore whose telephone number is (571)270-7313. The examiner can normally be reached on Monday through Thursday between 8:30 a.m. and 4:00 p.m. eastern time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Travis Pogmore/
Examiner, Art Unit 2436

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436